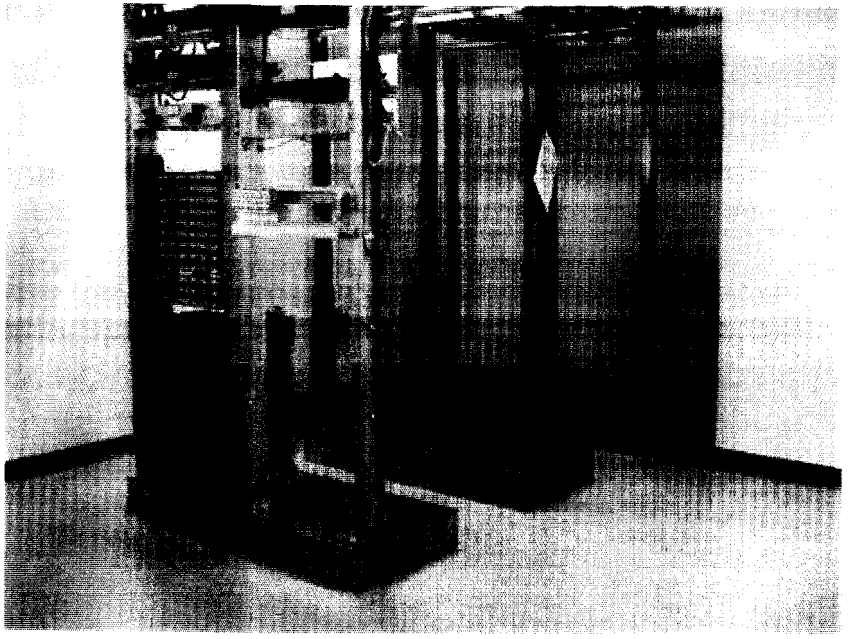
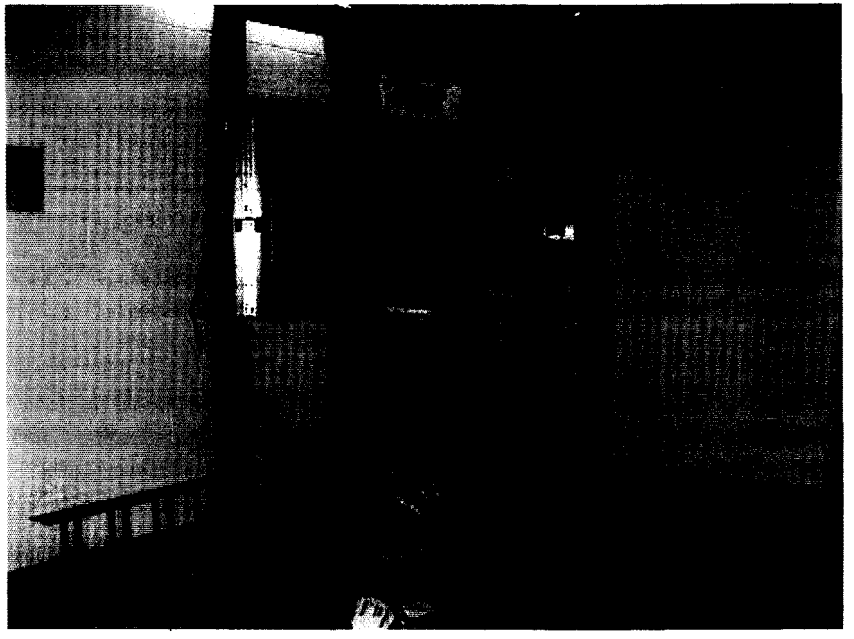
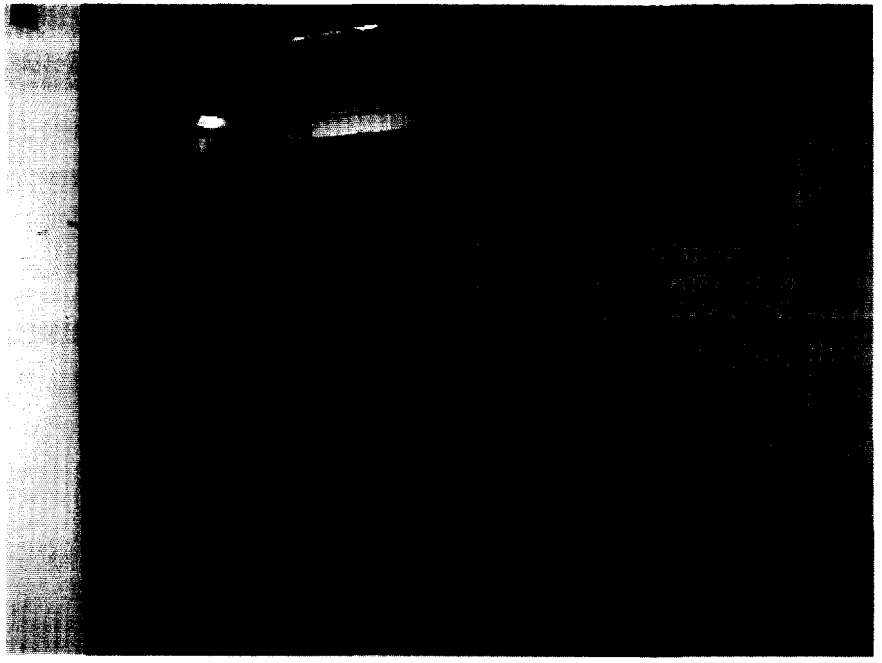
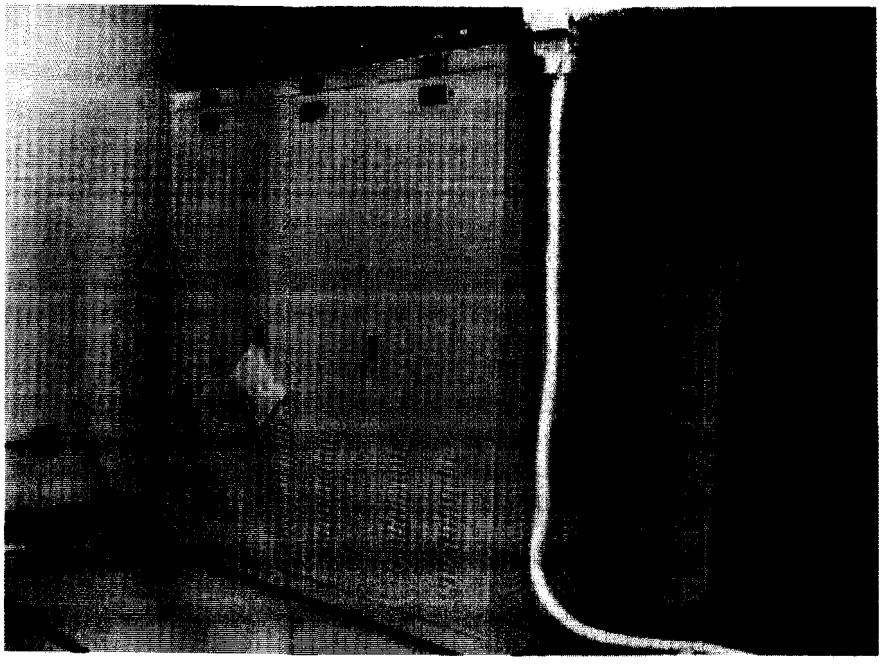
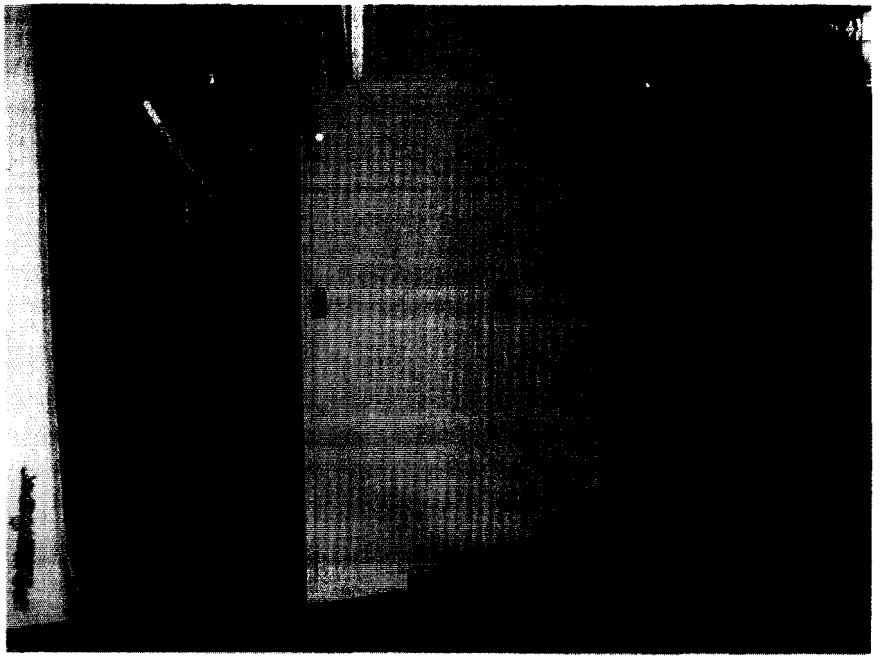










Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

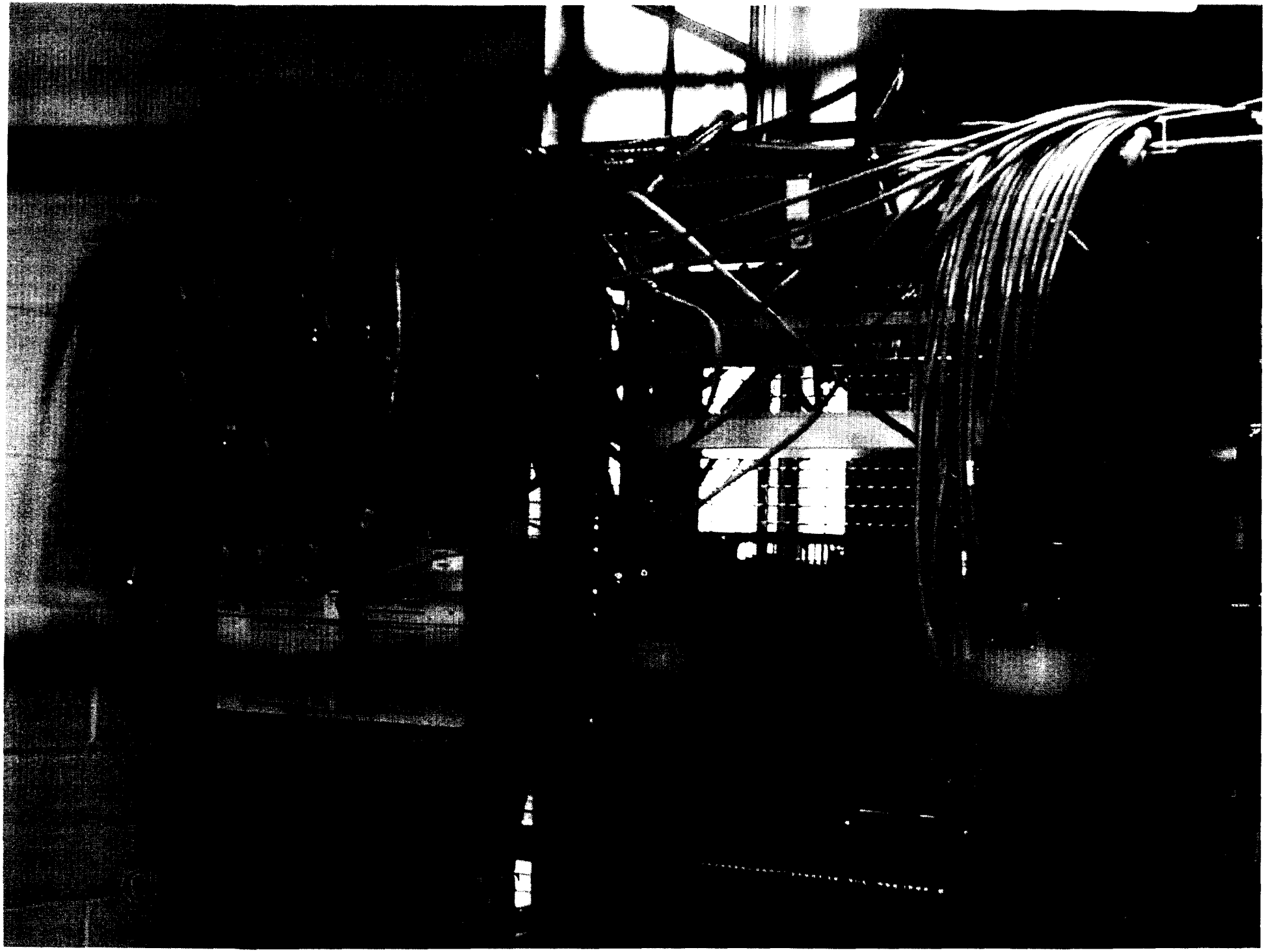
In the Matter of	)	
	)	
Deployment of Wireline Services Offering Advanced Telecommunications Capability	)	CC Docket No. 98-147
	)	
and	)	
	)	
Implementation of the Local Competition Provisions of the Telecommunications Act of 1996	)	CC Docket No. 96-98

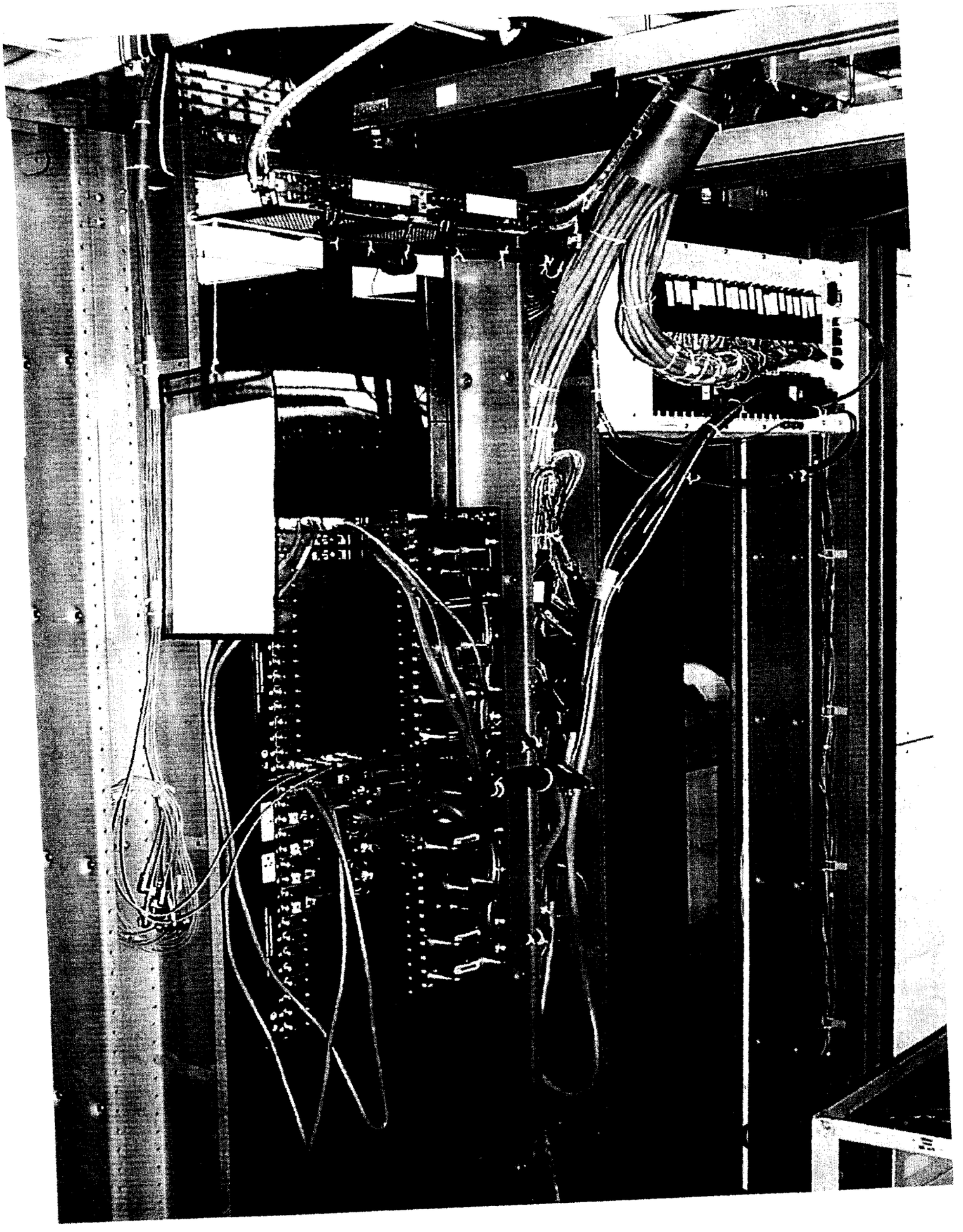
ATTACHMENT B-5 TO THE DECLARATION OF MICHAEL D. POLING

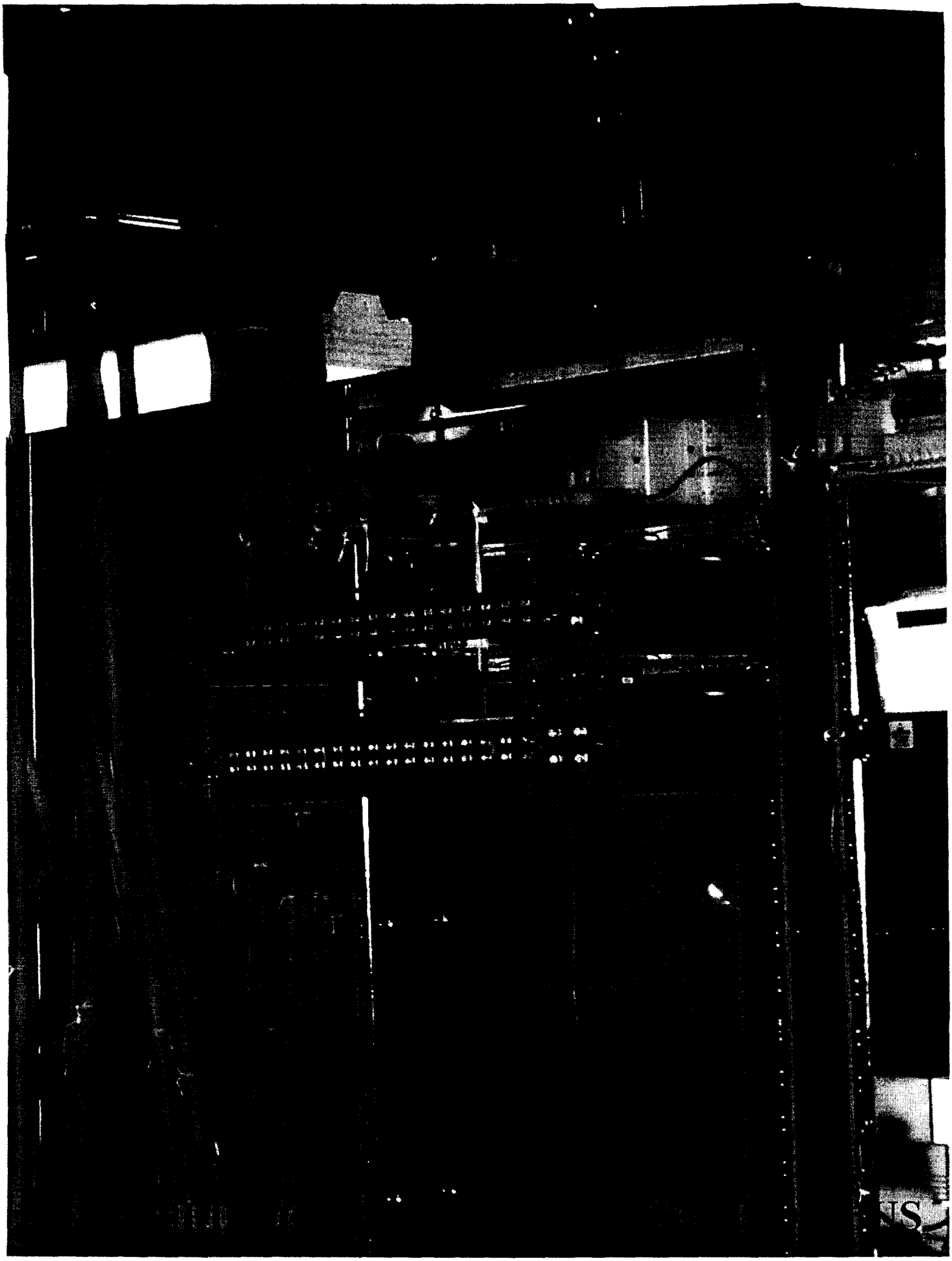
1. The carriers collocating at Verizon's central offices must adhere to the same safety standards that Verizon expects of its own vendors. These safety standards include Telcordia's Network Equipment and Building Specifications ("NEBS") for the installation of equipment in a central office environment. As the number of collocation arrangements continues to increase, Verizon is beginning to experience an increased deterioration in the overall quality installation work performed by the carriers.

2. The Exhibits to this attachment provide examples of cabling arrangements that are typical of many of the installation jobs in collocation areas. This quality of work in a commingled environment where collocator equipment was in the same bay as Verizon's would cause major problems in accessibility to equipment within the same general area. In addition, it would lead to increased opportunities for accidental dislodging of connections. In a segregated environment, such installations do not impact Verizon's network, so long as the installation meets NEBS and other safety standards.

However, commingling would put Verizon in the position of either supervising the quality of collocator installations or sacrificing the reliability of its own network.







ATTACHMENT C

ATTACHMENT C

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	
Deployment of Wireline Services Offering Advanced Telecommunications Capability	CC Docket No. 98-147
and	
Implementation of the Local Competition Provisions of the Telecommunications Act of 1996	CC Docket No. 96-98

DECLARATION OF DAVID G. MAPLES, III

1. My name is David G. Maples, III. I am a Vice President and Director in the Atlanta office of Investigative Group International, Inc. ("IGI"), responsible for, among other things, security management. My business address is 3423 Piedmont Road, NE, Suite 505, Atlanta, Georgia 30305. I have prepared this declaration to analyze the effect of the Commission's proposed collocation rules on an incumbent local exchange carrier's ("ILEC's") ability to maintain security in its central office.

I. BACKGROUND AND EXPERIENCE

2. Prior to joining IGI, I worked for the Federal Bureau of Investigation ("FBI") for 26 years. While there, I supervised the FBI's Organized Crime Squad, its Counter-Terrorism Program and its Major Case Squad in Los Angeles.

3. Since joining IGI, I have conducted security surveys for several corporate clients. For example, I assessed the security of the New York offices of a

prominent investment banking and securities trading firm, and conducted security surveys of the principal officers' residences. Further, I have coordinated security surveys for an internet-based health information services provider and for a telecommunications and information services holding company. These security surveys examined the firms' security measures (such as alarms, locks and electronic access control) and the firms' ability to secure proprietary information, property and personnel. I am currently working to identify vulnerable areas and to make recommendations regarding physical security, access control and proprietary information protection for a large Washington, D.C. law firm.

II. PURPOSE & SUMMARY OF AFFIDAVIT

4. I submit this testimony in response to the Commission's request for comments on whether ILECs should be required to place CLEC equipment in any pocket of space in an ILEC central office, including in close proximity to, or in the same bay as, the ILEC's equipment, without the ability to partition or otherwise segregate the CLEC's equipment from the ILEC's equipment. (I refer to this as "commingling.") The FCC has also sought comments on the security issues raised by permitting collocation at remote terminals, which are free-standing structures located outside of the central office that house telecommunications equipment.

5. To prepare this Declaration, I visited four central offices in the Washington, DC metropolitan area, including a large office in the District of Columbia, two medium-sized offices in Virginia and a small, rural office in Maryland, as well as a remote terminal in Virginia. Several Verizon managers accompanied me on these tours to give me a sense of the challenges Verzon would face in a "commingled" environment.

I also had numerous discussions over a number of weeks with various Verizon personnel from the Corporate Security organization regarding the security issues facing Verizon.

6. My Declaration addresses the significant security risks associated with commingling CLEC and ILEC equipment. In my opinion, Verizon would be exposed to intentional and unintentional damage to its network and equipment if it were required to commingle collocator equipment with its own. It is also my opinion that cameras and card readers would not adequately protect Verizon from these risks, and in any event, would be prohibitively costly to implement. Finally, I believe that the security risks, including the risks to network integrity and reliability, associated with permitting collocators unrestricted access to remote terminals are even greater because it would be virtually impossible to secure Verizon's equipment adequately or to determine who was responsible for damaging or pilfering the equipment within remote terminals because Verizon employees are not present at these premises.

7. After reviewing the various collocation options and visiting Verizon central offices, I have concluded that Verizon can only be assured full network security if competitors are located in separate and partitioned areas of the central office.

8. In Section III below, I address the various kinds of risks Verizon (and its customers) would face in a commingled environment. I discuss the effectiveness of various security methods in Section IV. These points are further demonstrated in the pictures included in Attachment C-1. Finally, I describe in Attachment C-2 the security measures (and associated costs) that would be required in a typical central office if Verizon were prohibited from partitioning its equipment.

III. THE SECURITY RISKS FACED BY VERIZON IN A COMMINGLED ENVIRONMENT ARE REAL AND THREATEN THE ENTIRE TELECOMMUNICATIONS NETWORK.

9. If Verizon is not permitted to separate or partition CLEC equipment, then the CLEC employees will have unlimited access to Verizon's equipment and network. (Mr. Poling explains in his Declaration that placing locked cabinets around Verizon's equipment is not possible.) In my opinion, accidents and sabotage are likely, if not highly probable, in the commingled environment contemplated by the FCC. Such an environment presents unique challenges from a security perspective. Put simply, requiring Verizon to commingle CLEC equipment with its own equipment creates significant risks for Verizon, its customers, and the communities served by Verizon's central offices.

A. VARIOUS FACTORS MAKE VERIZON'S CENTRAL OFFICES VULNERABLE TO SECURITY THREATS.

10. It is important to understand the characteristics and configurations of Verizon's central offices to assess the significant security risks Verizon would face in a commingled environment. Verizon's central offices were designed to house telecommunications equipment; they were ***not*** designed to handle the unique security challenges raised by the presence of CLECs in these offices.

11. For example, Verizon's central offices contain numerous line-ups of equipment that are typically 7' high, 26" wide and 12" deep, depending on the size of the equipment within the line-up. Verizon's central offices also contain more sensitive equipment, including power and other infrastructure equipment such as main distributing

frames, and so forth, which are located in scattered areas throughout the central office. Verizon's 911 switches and tandem switches may also be located on the same floorp.

12. Exhibit 1 to Attachment C-1 shows a typical equipment line-up, with some bays full and some bays empty. This equipment, which now serves live customers, has been placed throughout Verizon's central offices over time. As a result, small pockets of space may exist near certain pieces of equipment – *e.g.*, in the middle of the room next to a 911 switch – that would be impossible to secure. In other words, because Verizon's central offices were not developed with the CLECs' commingling proposal in mind, but instead evolved over time with equipment being placed where it made the most technical sense, this new proposal presents security difficulties.

13. Verizon's central offices were not designed to accommodate multiple carriers and the security risks associated with commingling CLEC and ILEC equipment. When Verizon built its offices, the structure itself was the primary security measure since only authorized personnel within Verizon were given access to these facilities. Indeed, most businesses and even the FBI regard the building perimeter as their chief way to keep unauthorized individuals out. If new offices were built today, Verizon could design them with interior security in mind, and for example, place all of its sensitive equipment on one floor, and leave other parts of the central office with empty space for collocators. Or Verizon could ensure that all the empty space in the central office was near a door that could be adequately secured. Unfortunately, these ideal configurations do not exist in Verizon's central offices today.

14. Another factor that makes Verizon's central offices vulnerable to security threats is that fact that there are often only a few, if any, Verizon employees

located in a central office at a particular time. And many Verizon central offices are totally unmanned for most of the day. As a consequence, it is unlikely that Verizon could prevent intentional or accidental damage to its equipment caused by a CLEC if it were not permitted to partition its equipment.

15. Indeed, commingling would increase exponentially the number of people with access to Verizon's equipment and therefore increase the likelihood of intentional or unintentional damage. Some central offices have more than twenty collocators, and each CLEC, in turn, has perhaps dozens of employees that would potentially have access to Verizon's central offices. No Verizon employee – even if he/she were in the central office at the same time as the CLEC employees – would be able to determine who belonged in the office and who did not, or on which piece of equipment a given technician was authorized to work.

16. These factors expose Verizon's central offices to the risks discussed below.

B. ACCIDENTS ARE LIKELY TO OCCUR WITH GREATER TRAFFIC.

17. Accidents and unintentional damage to equipment are highly likely in the commingled environment urged by the CLECs. As Exhibits 5 and 6 to Attachment C-1 demonstrate, equipment aisles are quite narrow and a CLEC technician may inadvertently touch and affect the equipment around him/her. While the same may be said of Verizon's own employees/agents, they have greater incentive to take care when working around this highly sensitive and costly equipment, and are more familiar with the environment in a given office. I discuss in more detail below the differences between Verizon's employees/agents and the CLECs' employees/agents.

18. Indeed, the CLECs have already demonstrated careless disregard for Verizon's rules and regulations, including rules designed to protect network equipment. For example, I was told that CLECs repeatedly ignore signs warning them not to use cellular phones in the central office because of the damage the emitted radio signals can do. Blatant and intentional breaches of Verizon's rules and regulations would have greater consequences if CLECs are permitted access to the more critical and sensitive pieces of network equipment located in the central office.

C. INTENTIONAL DAMAGE TO, OR THEFT OF, VERIZON'S EQUIPMENT IS LIKELY AND WOULD HAVE FAR-REACHING EFFECTS.

19. Sabotage, intentional damage and theft are more likely in a commingled environment. Although most CLEC employees/agents are honorable, the stark reality is that some people will always refuse to abide by the rules. As Mr. Poling explains, Verizon has documented numerous security violations by CLEC employees. ***See*** Poling Declaration, Attachment B-1. These security violations demonstrate that CLEC employees often blatantly disregard security rules, or are simply careless. The consequences of such violations will be even more serious if Verizon is denied the ability to protect its network with partitioning.

20. Verizon's interest in protecting itself against the threat of sabotage, intentional damage to its network, or theft is not sinister or anticompetitive, but simply smart corporate management. In my 26 years at the FBI, I saw numerous examples of corporate sabotage in a variety of circumstances. Verizon's desire to secure its network is no different from the interests of the many corporate clients I have worked with in my career at IGI.

21. Disrupting service in a particular central office could also put lives at risk. Many of Verizon's central offices house tandem switches and provide 911 services, and others house the Signal Transport Point ("STP") switches, which are the lifeline to numerous subtending switches. If these switches were damaged, or the central offices housing these switches were otherwise comprised, lives could be lost and financial implications to major businesses could stretch into the many millions of dollars.

22. There would be many opportunities for a CLEC employee/agent to steal or intentionally damage Verizon's equipment. During my visits to the various Verizon central offices, I saw a great deal of equipment left out in the open. For example, I saw numerous unsecured test sets and computers in each central office. (*See* Exhibits 3 and 7 to Attachment C-1). Verizon personnel explained that often this equipment – which I was told costs well into the tens of thousands of dollars – must be left out in the open to run continuous 24- or 48-hour tests. Because CLECs use this same equipment, the risk exists for a CLEC employee to steal it, either to use it or to sell it on the black market. Although much of this equipment is industry-specific, it would easily be disposed of given the growing number of companies in the domestic and foreign telecommunications industry. Finally, much of this equipment consists of desktop and laptop computers – equipment that is used every day by the general population. (See Exhibits 3 and 7 to Attachment C-1).

23. In addition to using the same test sets as Verizon, CLECs also use the same types of plug-in cards, which as the name implies, can be unplugged easily and placed in an individual's pocket.[1] (*See* Exhibit 5 to Attachment C-1). It would be

[1] Verizon personnel explained to me that these cards cost well into the thousands of dollars.

virtually impossible to recover stolen plug-in cards because they are so prevalent in the industry.

24. Moreover, in a commingled environment, CLECs would have access, in smaller offices, to the cable vault and manhole, where a single cut cable would disrupt service to tens of thousands of customers. The ramifications are staggering.

25. Given my experience at the FBI, the FCC must also consider the greater chance that a CLEC employee would intentionally or unintentionally damage Verizon's equipment because such damage would harm Verizon, but not the CLEC. Verizon employees explained on my visits to the central offices that there is a great deal of Verizon equipment that could be put out of service without affecting the CLECs' service – e.g., Verizon's transmission equipment. Therefore, it is incorrect to assume that a CLEC employee would exercise the same degree of care to prevent damage to Verizon equipment that a Verizon employee would exercise. In fact, incidents of accidental as well as intentional damage to Verizon's equipment in a collocated environment have already occurred, as Mr. Poling points out in his Declaration.

26. The FCC must also consider that some CLECs, I have been told, have hired former Verizon employees, some of whom may been disgruntled or who may have left for other reasons that would make them have less concern for the well-being of Verizon's network. This fact makes the potential for intentional or unintentional damage even more likely in my opinion.

27. It is also possible that a CLEC could be compromised by an outside entity that understood the damage that could be done to the U.S. government or economy by damaging a given central office. Although it is possible that these entities

could also infiltrate Verizon, the risk would increase exponentially in a commingled environment due to the large increase in the number of CLEC employees/agents – people not hired or screened by Verizon – who would have access to Verizon's network. In addition, as I explain below, CLEC employees have given their access cards to other CLEC employees not authorized to enter Verizon's central offices.

D. CONFIDENTIAL AND PROPRIETARY INFORMATION COULD BE COMPROMISED IF CLECS ARE PERMITTED TO COMMINGLE THEIR EQUIPMENT.

28. Permitting CLECs to commingle their equipment could compromise sensitive, confidential and proprietary information, including law enforcement investigations. For example, the offices that I visited housed facilities serving various federal government agencies, as well as local governments. Disrupting service (both voice and data) to these agencies could compromise national and local interests.[2] Further, several government agencies have offices located in various office buildings and do not want their locations known to the public. Equipment serving these agencies, however, displays common language codes and circuit identifications, which are tied to customer names, addresses and detailed service descriptions in Verizon's databases. The CLECs can easily access this information in a commingled environment and therefore compromise the security of these government agencies.

29. Permitting the CLECs free access to Verizon's network could also jeopardize other types of law enforcement efforts. For example, as I understand, from

[2] A federal task force was specifically created to monitor, among other things, the security of the telecommunications infrastructure. (http://www.nipc.gov) Verizon should, at a minimum, be permitted to deny CLECs access to the portions of central offices serving the White House, FBI or other highly sensitive agencies, unless these agencies authorize the CLECs to have access to this equipment.

discussions with Verizon personnel, that most wiretap monitoring today can be accomplished by placing small pieces of equipment in central offices and remote terminals. While central office wire-tapping equipment has become somewhat more difficult to distinguish from ordinary central office equipment, this equipment could still be identified by an astute CLEC employee, particularly equipment located in remote terminals. In a commingled environment, the number of individuals with access to this information would increase exponentially, increasing the chance that the someone will tip of the target of the investigation.

30. In addition, CLECs with free access to Verizon's network would also have access to sensitive corporate marketing information. Much of Verizon's equipment displays proprietary business information, including the name and location of corporate clients and the type of service they have ordered from Verizon. A CLEC with free reign in Verizon's offices could easily obtain this valuable marketing information to solicit new business.

31. In short, it is clear that forcing ILECs to commingle CLEC equipment may have dire and unintended consequences. The FCC must carefully protect the security and integrity of the telecommunications network. In my opinion, permitting ILECs to partition off their networks from unfettered access by CLECs is the only reasonable and effective solution.

E. THE PRESENCE OF CLEC EMPLOYEES/AGENTS IN VERIZON'S CENTRAL OFFICES PRESENTS DIFFERENT SECURITY ISSUES THAN VERIZON'S OWN EMPLOYEES/AGENTS.

32. Several CLECs have argued that CLEC employees/vendors are no different from Verizon employees/vendors and should be provided the same access to the

network. I disagree. For the reasons discussed below, there are real and significant differences between these groups that raise security concerns.

33. First, unlike Verizon's own employees, CLECs' employees are not accountable to Verizon. As a consequence, Verizon has no recourse against a CLEC employee who intentionally, or unintentionally, damages or pilfers Verizon's equipment, or who blatantly violates security guidelines. While Verizon may escort the CLEC employee out of the central office, Verizon may not fire the employee as it would its own employee or vendor. The CLEC employee, moreover, may simply re-enter Verizon's central offices at another time using someone else's access card or may accompany a co-worker with a valid access card. Indeed, I witnessed first-hand three CLEC employees entering a Verizon central office, only one of whom had a valid access card. (I describe this incident in more detail below). This total inability to punish a CLEC agent/bad actor is a key factor that the Commission must take into account in determining whether it should permit Verizon to secure its network with partitioning material. Moreover, a Verizon employee working in a given central office is likely well known by his/her co-workers. In my opinion, these differences require the complete separation of CLEC equipment from Verizon's equipment.

34. Second, while Verizon is permitted to escort its own vendors, the FCC has determined that Verizon may not escort CLEC technicians and vendors. And while Verizon may require its own vendor to access Verizon's central offices only at a particular time and upon prior notice, Verizon must permit the CLECs to access its equipment in the central office 24 hours a day, seven days per week. Because the CLECs

have unlimited access, and do not require Verizon's prior approval to enter the central office, Verizon must be permitted to separate and secure its own equipment.

35. Third, as noted above, Verizon has no way of knowing whether the CLEC employee has been adequately trained to work on equipment in a central office environment. By contrast, Verizon's own employees undergo significant training before they are permitted to work in the central office. If the FCC requires Verizon to commingle CLEC equipment, then Verizon will be exposed to the risk that an untrained CLEC employee/agent may accidentally damage Verizon's equipment while working on the CLEC's equipment, or may inadvertently work on Verizon's equipment.

36. Fourth, CLEC employees have a significantly lower incentive to follow proper procedures and work carefully around Verizon's equipment. Verizon's employees and vendors, on the other hand, have the incentive to work carefully around Verizon's equipment for fear of losing their jobs or contracts.

37. Finally, the CLECs are Verizon's competitors. As noted, the business reality is that some CLEC employees will attempt to sabotage or steal Verizon's equipment.

38. Because of these fundamental differences between CLEC employees/agents and Verizon employees/agents, Verizon would face serious security problems if it were prohibited from partitioning its equipment.

IV. PARTITIONING IS THE ONLY EFFECTIVE SECURITY METHOD.

39. In this section I address the CLECs' argument that security cameras provide sufficient security, and that Verizon should not be permitted to partition its equipment. As I explain below, the CLECs are wrong. Partitioning provides the only

truly effective method of securing Verizon's network from the risks addressed in Section II.

40. There are four levels of security measures that are feasible in a central office environment: (i) those which record events; (ii) those which control access; (iii) those which act as a deterrent; and (iv) those which prevent breaches from occurring.

A. PARTITIONING EFFICIENTLY USES SPACE AND IS COST EFFECTIVE.

41. Given the highly sensitive nature of the equipment in a central office and the far-reaching effects of a network outage, Verizon should, from a security perspective, be permitted to implement the last alternative – that is, security measures that actually prevent breaches from occurring. Plainly, partitioning Verizon's central office is the only way to prevent security breaches. Moreover, as Exhibit 2 to Attachment C-1 demonstrates, partitioning is non-intrusive and uses space efficiently. It is also the most cost-effective security method.

42. It is not possible to partition commingled CLEC and ILEC equipment, as Exhibit 1 to Attachment C-1 demonstrates. I have been told that lockable cabinets do not exist that can be placed around Verizon equipment that is located in the same rack or bay with CLEC equipment. And even if such cabinets existed, it would not be economically feasible to protect all of the equipment in a central office in this manner. This is also addressed in Mr. Poling's Declaration.

43. Other types of preventative security measures are not practical. For example, it would be cost prohibitive to place security guards at all of Verizon's 5,500 central offices, 24 hours per day. This would require a work force of

approximately 22,000 new employees (four guards per central office, or one per shift). This plainly is not a workable option.

B. CAMERAS DO NOT PROVIDE ADEQUATE SECURITY.

44. Security cameras, which in theory sound like a good solution, are ineffective as a general rule based on my experience. Cameras cannot prevent accidents or damage from occurring, nor do they provide a reliable audit trail.

45. Real-time monitoring of cameras, for example, is not a viable option. In my experience, this method of security, which was used rather ineffectively at the Olympic games, is almost entirely useless and has no relation to its portrayal in the media and on television. Two scenarios may occur: a person is required to monitor either upwards of fifteen screens, or a single screen whose image flickers among several camera feeds. In the first example, no one can effectively monitor that many screens. Moreover, the number of people that would be required to monitor the screens necessary for an entire central office is staggering. In the second scenario, a monitor looking at a single screen is likely to miss activity because of the constantly changing camera angles. (I address below the fact that it would be impossible, in any event, to capture every angle of the central office.) In either case, my experience is that after approximately one hour of one day, the monitor's attention span evaporates and he/she is highly unlikely to notice any illegal activity on the screen(s).

46. Moreover, even if real time camera monitoring were effective, it would not *prevent* incidents from occurring, unless Verizon posted a guard in every central office to monitor the camera(s) and to be ready to stop an illegal or disruptive

action. As explained above, posting a guard in each Verizon central office (or remote terminal) is not a reasonable option.

47. Nor do cameras provide a sufficient deterrent effect, although they are useful in limited circumstances. First, no camera array can reasonably cover every square inch of a physical facility, especially in an environment like a central office where tall equipment bays and bulky equipment block many parts of the office from view. Indeed, as Exhibit 1 to Attachment C-1 demonstrates, because of tall equipment line-ups, Verizon would have to install multiple cameras in each equipment line-up to capture the relevant activities. To further demonstrate this point, Verizon analyzed a typical central office and determined that it would need nearly 100 cameras to cover every potential angle of the central office – a very costly approach. *See* Attachment C-2.

48. Second, even if Verizon installed enough cameras to capture every angle in a central office, the quality of the picture simply would not be sufficient to capture the precise movements of a CLEC technician working on central office equipment, and may not even be sufficient to determine the piece of equipment being worked on by the technician. (*See* Exhibit 5 to Attachment C-1). This is explored in greater detail in Attachment C-1.

C. CARD READERS ALONE ARE NOT EFFECTIVE.

49. Security card readers, in place in the Verizon offices I visited, are equally ineffective at accomplishing their intended purposes of providing an audit trail of visitors and controlling access, although of course, they provide some measure of security when combined with another method of security, for example fencing or cameras. First, the owner of an access card linked to a bad act can always plausibly deny that he/she

committed the bad deed by claiming that someone else used the card or that some other person present in the office accomplished the bad deed. Although Verizon could aim a camera at the front door, for the reasons discussed above, this would not prevent incidents from occurring. In addition, card readers do not indicate when CLECs "tailgate" other CLECs or vendors, *i.e.*, walk in behind them without swiping an access card across the reader.

50. Security access cards are intended to prevent unauthorized personnel from accessing certain sections of the central offices and to provide Verizon with a record of who enters its offices. (Card readers cannot relate when a person leaves an office, thus making it impossible to determine the duration of a CLEC's stay and thus if he/she was in the office when a security breach occurred.) Verizon, however, has documented numerous instances of CLEC employees and representatives using access cards belonging to others, rendering the cards utterly useless. Moreover, access cards, if used properly, provide Verizon only with a witness or suspect for accidents or intentional bad acts. They cannot act as a preventative measure, nor can they help Verizon positively identify a bad actor.

51. To cite a real-world example, while I was touring one central office three CLEC employees entered the collocation room. Only one had an identification badge and access card. The other two individuals had no identification badge or access card. I have been told that this happens frequently.

52. Moreover, at many central offices, secondary exits are not monitored since they serve solely as exits. It would be entirely possible for a CLEC to enter and let in unauthorized personnel by holding open the secondary exits. In fact,